Internet et droits humains, il y a vraiment un rapport ? (1/13)

Stéphane Bortzmeyer
stephane+breizhcamp@bortzmeyer.org

21 mars 2019

Petit rappel sur l'Internet

Petit rappel sur l'Internet

- Les données sont découpées en datagrammes, chaque datagramme comportant un en-tête et un corps, l'en-tête inclut les adresses IP de source et destination, chacune faisant 128 bits, la fiabilité des données étant assurée par un protocole de transport qui gère accusés de réception, réémission...

Petit rappel sur l'Internet

- Les données sont découpées en datagrammes,
- Non, en fait, on s'en fout,

Petit rappel sur l'Internet

- Les données sont découpées en datagrammes,
- Non, en fait, on s'en fout,
- Ce qui est important, dans l'Internet, ce n'est pas TCP/IP ou le datagramme,

Petit rappel sur l'Internet

- Les données sont découpées en datagrammes,
- Non, en fait, on s'en fout,
- Ce qui est important, dans l'Internet, ce n'est pas TCP/IP ou le datagramme,
- Internet est un réseau de réseaux, un protocole commun est utilisé, à tous les niveaux de la connectivité, entre opérateurs, ou bien entre client et opérateur,

Petit rappel sur l'Internet

- Les données sont découpées en datagrammes,
- Non, en fait, on s'en fout,
- Ce qui est important, dans l'Internet, ce n'est pas TCP/IP ou le datagramme,
- Internet est un réseau de réseaux, un protocole commun est utilisé, à tous les niveaux de la connectivité,
- Il n'y a pas de distinction entre accès et service, du moment qu'on a accès, on peut fournir des services (« l'imprimerie a permis au peuple de lire, l'Internet lui permet d'écrire »),

Petit rappel sur l'Internet

- Les données sont découpées en datagrammes,
- Non, en fait, on s'en fout,
- Ce qui est important, dans l'Internet, ce n'est pas TCP/IP ou le datagramme,
- Internet est un réseau de réseaux, un protocole commun est utilisé, à tous les niveaux de la connectivité,
- Il n'y a pas de distinction entre accès et service, du moment qu'on a accès, on peut fournir des services,
- Les intermédiaires sont facultatifs,

Petit rappel sur l'Internet

- Les données sont découpées en datagrammes,
- Non, en fait, on s'en fout,
- Ce qui est important, dans l'Internet, ce n'est pas TCP/IP ou le datagramme,
- Internet est un réseau de réseaux, un protocole commun est utilisé, à tous les niveaux de la connectivité,
- Il n'y a pas de distinction entre accès et service, du moment qu'on a accès, on peut fournir des services,
- Les intermédiaires sont facultatifs,
- Il y a une forte culture de l'innovation sans permission.

Petit rappel sur les droits humains

Petit rappel sur les droits humains

- Des droits **universels**, acquis à tout être humain,

Petit rappel sur les droits humains

- Des droits **universels**, acquis à tout être humain,
- Formalisés dans la DUDH (Déclaration Universelle des Droits de l'Homme),

Petit rappel sur les droits humains

- Des droits **universels**, acquis à tout être humain,
- Formalisés dans la DUDH (Déclaration Universelle des Droits de l'Homme),
- Un idéal, pas la description d'une réalité,

Petit rappel sur les droits humains

- Des droits **universels**, acquis à tout être humain,
- Formalisés dans la DUDH (Déclaration Universelle des Droits de l'Homme),
- Un idéal, pas la description d'une réalité,
- Très menacés, en fait et en droit,

Petit rappel sur les droits humains

- Des droits **universels**, acquis à tout être humain,
- Formalisés dans la DUDH (Déclaration Universelle des Droits de l'Homme),
- Un idéal, pas la description d'une réalité,
- Très menacés, en fait et en droit,
- Avoir un droit est une chose, pouvoir l'exercer réellement en est une autre.

Mais quel rapport entre les deux ?

Mais quel rapport entre les deux ?

- L'Internet est un outil, un outil est neutre, non ?

Mais quel rapport entre les deux ?

- L'Internet est un outil, un outil est neutre, non ?
- Le fait de pouvoir publier sur le Web peut permettre aussi bien Wikipédia que Breitbart,

Mais quel rapport entre les deux ?

- L'Internet est un outil, un outil est neutre, non ?
- Le fait de pouvoir publier sur le Web peut permettre aussi bien Wikipédia que Breitbart,
- Il faut séparer les discussions techniques et politiques.

Mais ce n'est pas aussi simple

Mais ce n'est pas aussi simple

- Le débat sur la neutralité de la technique est aussi ancien que la philosophie,

Mais ce n'est pas aussi simple

- Le débat sur la neutralité de la technique est aussi ancien que la philosophie,
- L'arme ne commet pas le meurtre, mais sans arme, le meurtre est moins facile.

Mais ce n'est pas aussi simple

- Le débat sur la neutralité de la technique est aussi ancien que la philosophie,
- L'arme ne commet pas le meurtre, mais sans arme, le meurtre est moins facile.
- « Nous façonnons nos outils, et ceux-ci à leur tour nous façonnent. » (McLuhan)

Mais ce n'est pas aussi simple

- Le débat sur la neutralité de la technique est aussi ancien que la philosophie,
- L'arme ne commet pas le meurtre, mais sans arme, le meurtre est moins facile.
- « Nous façonnons nos outils, et ceux-ci à leur tour nous façonnent. » (McLuhan)
- La technique ne nous dicte pas tout mais elle influence et oriente (des exemples concrets suivent).

Mais ce n'est pas aussi simple

- Le débat sur la neutralité de la technique est aussi ancien que la philosophie,
- L'arme ne commet pas le meurtre, mais sans arme, le meurtre est moins facile.
- « Nous façonnons nos outils, et ceux-ci à leur tour nous façonnent. » (McLuhan)
- La technique ne nous dicte pas tout mais elle influence et oriente.
- « Je veux faire des choix, pas des compromis. » ? ? ?

Mais ce n'est pas aussi simple

- Le débat sur la neutralité de la technique est aussi ancien que la philosophie,
- L'arme ne commet pas le meurtre, mais sans arme, le meurtre est moins facile.
- « Nous façonnons nos outils, et ceux-ci à leur tour nous façonnent. » (McLuhan)
- La technique ne nous dicte pas tout mais elle influence et oriente.
- « Je veux faire des choix, pas des compromis. » ? ? ?
- Un tutoriel en vidéo est un choix, le choix d'exclure les mal-connectés.

Exemple : l'usage du numérique laisse des traces

Exemple : l'usage du numérique laisse des traces

- Par défaut, le numérique laisse des traces : collecter des données n'est pas cher,

Exemple : l'usage du numérique laisse des traces

- Par défaut, le numérique laisse des traces : collecter des données n'est pas cher,
- Et le numérique permet de traiter ces traces,

Exemple : l'usage du numérique laisse des traces

- Par défaut, le numérique laisse des traces : collecter des données n'est pas cher,
- Et le numérique permet de traiter ces traces,
- Aller au restaurant sans donner son nom et payer en liquide ? Acheter un livre papier à une boutique physique et payer en liquide ?

Exemple : l'usage du numérique laisse des traces

- Par défaut, le numérique laisse des traces : collecter des données n'est pas cher,
- Et le numérique permet de traiter ces traces,
- Aller au restaurant sans donner son nom et payer en liquide ? Acheter un livre papier à une boutique physique et payer en liquide ?
- Encourager le numérique, c'est encourager la traçabilité,

Exemple : l'usage du numérique laisse des traces

- Par défaut, le numérique laisse des traces : collecter des données n'est pas cher,
- Et le numérique permet de traiter ces traces,
- Aller au restaurant sans donner son nom et payer en liquide ? Acheter un livre papier à une boutique physique et payer en liquide ?
- Encourager le numérique, c'est encourager la traçabilité,
- Exercice pour cours d'informatique : comment limiter la traçabilité.

Exemple : DHCP est trop bavard

Exemple : DHCP est trop bavard

- Pour avoir une adresse IP, votre machine annonce, à la cantonade, qui elle est, avec plein de détails, comme sa précédente adresse IP,

Exemple : DHCP est trop bavard

- Pour avoir une adresse IP, votre machine annonce, à la cantonade, qui elle est, avec plein de détails, comme sa précédente adresse IP,
- RFC 7819 et 7824,

Exemple : DHCP est trop bavard

- Pour avoir une adresse IP, votre machine annonce, à la cantonade, qui elle est, avec plein de détails, comme sa précédente adresse IP,
- RFC 7819 et 7824,
- Exercice pour cours d'informatique : lire les solutions du RFC 7844 (minimiser les informations envoyées). Discuter les conséquences sur l'administration système.

Exemple : trafic en clair par défaut

Exemple : trafic en clair par défaut

- Sur l'Internet, le trafic n'est pas systématiquement chiffré, ce qui facilite la surveillance,

Exemple : trafic en clair par défaut

- Sur l'Internet, le trafic n'est pas systématiquement chiffré, ce qui facilite la surveillance,
- On peut le chiffrer mais il faut souvent une action explicite $\longrightarrow$ tout le monde ne le fait pas.

Exemple : trafic en clair par défaut

- Sur l'Internet, le trafic n'est pas systématiquement chiffré, ce qui facilite la surveillance,
- On peut le chiffrer mais il faut souvent une action explicite $\longrightarrow$ tout le monde ne le fait pas.
- D'autres choix seraient possibles (voir par exemple le protocole HIP).

Exemple : trafic en clair par défaut

- Sur l'Internet, le trafic n'est pas systématiquement chiffré, ce qui facilite la surveillance,
- On peut le chiffrer mais il faut souvent une action explicite $\longrightarrow$ tout le monde ne le fait pas.
- D'autres choix seraient possibles (voir par exemple le protocole HIP).
- Exercice pour cours d'informatique : lister les avantages et les inconvénients du chiffrement systématique.

Exemple : les intermédiaires

Exemple : les intermédiaires

- Dans beaucoup de cas, Alice ne parle plus directement à Bob,

Exemple : les intermédiaires

- Dans beaucoup de cas, Alice ne parle plus directement à Bob,
- Mais via des intermédiaires « choisis » (serveur de courrier, serveur XMPP / Matrix, instance Fédivers, Facebook...) ou pas (routeur NAT, pare-feu...)

Exemple : les intermédiaires

- Dans beaucoup de cas, Alice ne parle plus directement à Bob,
- Mais via des intermédiaires « choisis » (serveur de courrier, serveur XMPP / Matrix, instance Fédivers, Facebook...) ou pas (routeur NAT, pare-feu...)
- Les intermédiaires peuvent être gentils ou méchants, mais ils ont toujours un pouvoir sur vous,

Exemple : les intermédiaires

- Dans beaucoup de cas, Alice ne parle plus directement à Bob,
- Mais via des intermédiaires « choisis » (serveur de courrier, serveur XMPP / Matrix, instance Fédivers, Facebook...) ou pas (routeur NAT, pare-feu...)
- Les intermédiaires peuvent être gentils ou méchants, mais ils ont toujours un pouvoir sur vous,
- Exercice pour cours d'informatique : lister les avantages et les inconvénients de l'utilisation d'intermédiaires.

Exemple : les techniques de rendez-vous

Exemple : les techniques de rendez-vous

- Pas sur le chemin, mais nécessaires pour mettre en contact Alice et Bob,

Exemple : les techniques de rendez-vous

- Pas sur le chemin, mais nécessaires pour mettre en contact Alice et Bob,
- Exemple typique : le DNS,

Exemple : les techniques de rendez-vous

- Pas sur le chemin, mais nécessaires pour mettre en contact Alice et Bob,
- Exemple typique : le DNS,
- Excellent endroit pour espionner et censurer (en Europe, le résolveur DNS menteur est la technique de censure la plus courante),

Exemple : les techniques de rendez-vous

- Pas sur le chemin, mais nécessaires pour mettre en contact Alice et Bob,
- Exemple typique : le DNS,
- Excellent endroit pour espionner et censurer,
- Exercice pour cours d'informatique : lister les avantages et les inconvénients des systèmes de rendez-vous.

Exemple : l'internationalisation

Exemple : l'internationalisation

- Postulat : toutes les langues (et toutes les écritures) se valent,

Exemple : l'internationalisation

- Postulat : toutes les langues (et toutes les écritures) se valent,
- Se limiter à l'alphabet latin est excluant, (a fortiori se limiter à l'ASCII),

Exemple : l'internationalisation

- Postulat : toutes les langues (et toutes les écritures) se valent,
- Se limiter à l'alphabet latin est excluant
- Protocoles et messages : on ne traduit pas le `GET` de HTTP,

Exemple : l'internationalisation

- Postulat : toutes les langues (et toutes les écritures) se valent,
- Se limiter à l'alphabet latin est excluant
- Protocoles et messages : on ne traduit pas le `GET` de HTTP,
- Mais on traduit ce que voit l'utilisateur,

Exemple : l'internationalisation

- Postulat : toutes les langues (et toutes les écritures) se valent,
- Se limiter à l'alphabet latin est excluant
- Protocoles et messages : on ne traduit pas le `GET` de HTTP,
- Mais on traduit ce que voit l'utilisateur,
- Exercice pour cours d'informatique : apprendre Unicode.

Exemple : DoH

Exemple : DoH

- Le DNS est très indiscret (RFC 7626),

Exemple : DoH

- Le DNS est très indiscret (RFC 7626),
- Projet « *DNS privacy* » à l'IETF : documenter, puis réduire le problème,

Exemple : DoH

- Le DNS est très indiscret (RFC 7626),
- Projet « *DNS privacy* » à l'IETF : documenter, puis réduire le problème,
- Parmi les solutions : chiffrer le trafic DNS (DoT, *DNS-over-TLS*) puis, pour éviter le blocage, DoH (*DNS-over-HTTPS*),

Exemple : DoH

- Le DNS est très indiscret (RFC 7626),
- Projet « *DNS privacy* » à l'IETF : documenter, puis réduire le problème,
- Parmi les solutions : chiffrer le trafic DNS (DoT, *DNS-over-TLS*) puis, pour éviter le blocage, DoH (*DNS-over-HTTPS*),
- Paul Vixie : « *i was surprised that the IESG was willing to allow a document to standardize hostility between me as a parent and my children who are subject to my parental controls technology, and between me as a network operator and malware authors who can't succeed without bypassing my DNS servers* » (bon exemple comme quoi les protocoles sont politiques),

Exemple : DoH

- Le DNS est très indiscret (RFC 7626),
- Projet « *DNS privacy* » à l'IETF : documenter, puis réduire le problème,
- Parmi les solutions : chiffrer le trafic DNS (DoT, *DNS-over-TLS*) puis, pour éviter le blocage, DoH (*DNS-over-HTTPS*),
- Paul Vixie,
- Faut-il aider à contourner la censure ?

Exemple : DoH

- Le DNS est très indiscret (RFC 7626),
- Projet « *DNS privacy* » à l'IETF : documenter, puis réduire le problème,
- Parmi les solutions : chiffrer le trafic DNS (DoT, *DNS-over-TLS*) puis, pour éviter le blocage, DoH (*DNS-over-HTTPS*),
- Paul Vixie,
- Faut-il aider à contourner la censure ?
- Exercice pour cours d'informatique : DoH est bon ou méchant ? IETF à Prague : réunion DoH le mardi 26 mars et *side meeting* le mercredi 27.

Conclusion et action

Conclusion et action

- Les problèmes politiques ne se règleront pas par la technique seule (« solutionnisme »),

Conclusion et action

- Les problèmes politiques ne se règleront pas par la technique seule,
- Mais l'action politique sans compréhension technique va faire n'importe quoi,

Conclusion et action

- Les problèmes politiques ne se règleront pas par la technique seule,
- Mais l'action politique sans compréhension technique va faire n'importe quoi,
- Il faut donc que les technicien·ne·s fassent de la politique et les citoyen·ne·s de la technique.

Conclusion et action

- Les problèmes politiques ne se règleront pas par la technique seule,
- Mais l'action politique sans compréhension technique va faire n'importe quoi,
- Il faut donc que les technicien·ne·s fassent de la politique et les citoyen·ne·s de la technique.
- Deux choses essentielles : « **il y a des choix** » et « **nous pouvons agir** »,

Conclusion et action

- Les problèmes politiques ne se règleront pas par la technique seule,
- Mais l'action politique sans compréhension technique va faire n'importe quoi,
- Il faut donc que les technicien·ne·s fassent de la politique et les citoyen·ne·s de la technique.
- Deux choses essentielles : « **il y a des choix** » et « **nous pouvons agir** »,
- *Keynote* de Bruce Schneier à la conférence RSA le 7 mars 2019 : « *We need public-interest technologists in policy discussions.* »,

Conclusion et action

- Les problèmes politiques ne se règleront pas par la technique seule,
- Mais l'action politique sans compréhension technique va faire n'importe quoi,
- Il faut donc que les technicien·ne·s fassent de la politique et les citoyen·ne·s de la technique.
- Deux choses essentielles : « **il y a des choix** » et « **nous pouvons agir** »,
- *Keynote* de Bruce Schneier : « *We need public-interest technologists in policy discussions.* »,
- Réunion *Public interest tech group* à l'IETF à Prague lundi 25 mars.